

Data Processing Agreement for EU customers

Effective date: March 10th, 2026

Version [11]

This agreement is drafted for the purposes of Article 28(3) of Regulation 2016/679 (the GDPR).

The parties have agreed on the following contractual clauses (the “**DPA**”) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subjects.

The following clauses are applicable even if the Data Controller in its processing of personal data is not bound by Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (“General Data Protection Regulation” or “GDPR”), if otherwise is not stated in the specific clause.

1. BACKGROUND

1. This DPA establishes the rights and obligations of the Data Controller and the Data Processor, when processing personal data on behalf of the Data Controller.
2. The DPA has been drafted to ensure the parties’ compliance with Article 28(3) of the General Data Protection Regulation.
3. In the context of the Service provided the Data Controller (as described in the Service Agreement entered into by the Parties), the Data Processor will process personal data on behalf of the Data Controller in accordance with this DPA.

2. RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR) and the applicable EU or Member State¹ data protection provisions. This clause is not applicable if the Data Controller is not bound by the GDPR.
2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
3. The Data Controller shall be responsible, inter alia, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. SCOPE OF PROCESSING

1. The Data Processor shall under the Agreement process personal data within the following framework:
 - The purpose of the Data Processor’s processing of personal data on behalf of the Data Controller is to provide the Service as described in the agreement between the Customer and the Data Processor. The Data Processor’s processing of personal data on behalf of the Data Controller shall mainly pertain to personal data obtained and stored on the platform provided as a service. At the platform, data subjects register and submit their data in the context of esports training and tournaments. The service is hosted and maintained by the Data Processor.
 - Personal data concerning data subjects using the platform will be processed. Such data will include the following: First and family name, email address, password, IP address, profile picture(s), biography,

¹ References to “Member States” made throughout the Agreement shall be understood as references to “EEA Member States” including the United Kingdom regardless of the outcome of “Brexit”.

game account, game journal, results and feedback. Data Processor will furthermore process any additional data that any data subject chooses to submit when using the platform.

2. The Data Processor shall process personal data only in accordance with documented instructions from the Data Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject. Subsequent instructions can be given by the Data Controller throughout the duration of the processing of personal data, but such instructions shall always be provided and kept in writing.
3. The Data Processor shall immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4. CONFIDENTIALITY

The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. SECURITY

1. Pursuant to Article 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
2. Pursuant to Article 32 GDPR, the Data Processor shall also, independently from the Data Controller, evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with information necessary to identify and evaluate such risks.
3. The Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor pursuant to Article 32 GDPR along with other information necessary for the Data Controller to comply with the Data Controller's obligation under Article 32 GDPR. If subsequently, in the assessment of the Data Controller, mitigation of the identified risks require further measures to be implemented by the Data Processor, than those already implemented by the Data Processor pursuant to Article 32 GDPR, the Data Controller shall in writing specify these additional measures to be implemented. This clause is not applicable if the Data Controller is not bound by the GDPR, insofar it relates to the Data Controllers compliance with the GDPR.
4. The Data Processor may be remunerated for the implementation of additional security measures hereto in accordance with the Service Agreement, subject to any such costs being approved in writing by the Data Controller in advance.

6. SUB-PROCESSORS

1. The Data Processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
2. The Data Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the DPA without the written authorisation of the Data Controller. The Data Processor shall inform in writing the Data Controller of any intended changes concerning the addition or replacement of sub-processors at least a week in advance, thereby giving the Data Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The list of sub-processors already authorised by the Data Controller are the following:

Organization Name	Role	Entity Country
Amazon Web Services, Inc.	Cloud hosting provider	United States
Edlink	Integrations provider	United States
Klaviyo, Inc.	Email delivery	United States
Sendgrid, Inc.	Email delivery	United States
Posthog Product	In-platform survey aggregator	United States
Functional Software, Inc. (Sentry.io)	Error logging	United States
Segment.io, Inc.	Communications services	United States
Crisp IM SAS	Customer support	France
Mixpanel	In-platform insights provider	United States
Clever	Integration provider	United States

3. Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in the DPA shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the DPA and the GDPR. The Data Processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to the DPA and the GDPR.
4. A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in the DPA are imposed on the sub-processor. Clauses on business-related issues that do not affect the legal data protection content of the sub-processor agreement, shall be excluded from submission to the Data Controller.
5. If the sub-processor does not fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR, in particular those foreseen in Articles 79 and 82 GDPR, against the Data Controller and the Data Processor, including the sub-processor.

7. ASSISTANCE TO THE DATA CONTROLLER

1. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR. This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:
 - a. the right to be informed when collecting personal data from the data subject
 - b. the right to be informed when personal data have not been obtained from the data subject
 - c. the right of access by the data subject
 - d. the right to rectification
 - e. the right to erasure ('the right to be forgotten')
 - f. the right to restriction of processing

- g. notification obligation regarding rectification or erasure of personal data or restriction of processing
 - h. the right to data portability
 - i. the right to object
 - j. the right not to be subject to a decision based solely on automated processing, including profiling
- 2. In addition to the Data Processor's obligation to assist the Data Controller, the Data Processor shall, taking into account the nature of the processing and the information available to the Data Processor, notify the Data Controller without undue delay, and in any event no later than 48 hours after becoming aware, of a personal data breach, in order to assist the Data Controller in ensuring compliance with:
 - a. The Data Controller's obligation to without undue delay and, where feasible, not later than 48 hours after having become aware of it, notify the personal data breach to the competent supervisory authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
 - b. the Data Controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
 - c. the Data Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
 - d. the Data Controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.
- 3. The Data Processor has right to remuneration for any assistance provided to the Data Controller in accordance with this clause 7, subject to any such costs being approved in writing by the Data Controller in advance.

8. ERASURE AND RETURN OF DATA

Upon termination of the provision of personal data processing services, the Data Processor shall be under obligation to return all the personal data to the Data Controller and delete existing copies unless Union or Member State law requires further storage of the personal data.

9. AUDIT AND INSPECTION

- 1. The Data Processor shall make available to the Data Controller information necessary to demonstrate compliance with the obligations laid down in Article 28 and the DPA and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.
- 2. The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

10. INDEMNITY

- 1. The Data Processor agrees to indemnify, keep indemnified and defend at its own expense, the Data Controller against all costs, claims, damages or expenses incurred by the Data Controller or for which the Data Controller becomes liable due to any failure by the Data Processor or its employees, subcontractors or agents to comply with any of its obligations under this DPA or the GDPR or any other applicable data processing legislation.

2. Data Processor is not liable for any indirect or consequential damages under this clause.

11. MISCELLANEOUS

1. The Customer shall ensure that the Data Subjects are provided the Privacy Policy as set out in Exhibit 2 b.
2. The DPA shall be interpreted in accordance with Swedish law without regard to its provisions covering conflict of laws. This shall not hinder a party or a third-party acting on behalf of the party from claiming compensation due to an arbitration award in the jurisdiction that governs the other party's assets and in accordance with the laws of that jurisdiction.
3. Any dispute, controversy, or claim that has not been amicably settled by the parties arising out of or in connection with the DPA or the breach, termination, or invalidity thereof, shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce (the "SCC"). The Rules for Expedited Arbitrations shall apply, unless the SCC in its discretion determines, taking into account the complexity of the case, the amount in dispute, and other circumstances, that the Arbitration Rules shall apply. In the latter case, the SCC shall also decide whether the Arbitral Tribunal shall be composed of one or three arbitrators.
4. The seat of arbitration shall be Stockholm, Sweden and the language of the arbitral proceedings shall be English.
5. All information disclosed during or otherwise in connection with the arbitral procedure including details of the arbitration proceeding, the arbitration award, settlement, or settlement awards shall be considered confidential information. This shall not prevent a party from seeking compensation due to an arbitration award in the jurisdiction that governs the other party's assets.

12. TERM

The Clauses shall become effective upon acceptance by the Data Controller, be it oral, written, or otherwise. The DPA shall be effective for the duration of the provision of personal data processing services.